RiskCAT 61508

Requirements derivation from Risk classes

A Tool of the

***C*ode *A*nalyzer *T*ool *S*et**

User's Manual

Günter Glöe & Ernst-Ulrich Mainka, Hamburg
www.cats-tools.de

Contents

1 OVERVIEW 1

2 INSTALLATION / FIRST START / DEINSTALLATION 4

2.1 The components of RiskCAT 4

2.2 Local Operation on a PC 4

2.3 Uninstallation on a local PC 5

2.4 Network Installation of RiskCAT 5

3 BASICS 6

3.1 Screen parts 6

3.2 Interrelationship between the screen parts 7

3.3 Measure states 7

3.4 Measure colours 7

3.5 Structure of the measures presentation used with RiskCAT 8

4 TASKS 9

4.1 Selection of risk parameters 9

4.2 Evaluation of Safety Integrity Level based on the risk parameters selected 9

4.3 Manual pre selection of the Safety Integrity Level 10

4.4 Structured overview on the recommended measures 10

4.5 Selection of individual measures 10

4.6 Selection of groups of measures according to the degree of obligation 11

4.7 Selection of measures related to documents 12

4.8 Selection of measures related to activities (life cycle phases) 13

4.9 Selection of measures related to key words 13

4.10 Copying the actually marked measure into the clipboard 13

4.11 Edit notes to the marked measure 14

4.12 Overview on defined terms in the measures texts 15

4.13 Retrieval in the original standards 16

4.14 Context related retrieval in the original standards 17

4.15 The context related presentation of explanations to the clause provided by IEC 61508 itself 18

4.16 The context related presentation of terms used in the measure texts given in IEC 61508, part 4 19

4.17 Project (session) storage in a file 20

4.18 Project (session) reload from a file 20

4.19 Result storage as RTF-file 20

5 MENU FUNCTIONS 22

5.1 "File" menu 22

5.2 "Standard Text" menu 22

5.3 "Help" menu 22

6 IEC 61508 SPECIFIC FEATURES 23

6.1 Presentation of the degree of obligation of the requirements 23

6.2 About the license for the standards supplied with RiskCAT 24

6.3 About some Key-Words in the individual measure presentation in RiskCAT 24

6.4 About the Safety Integrity Level (SIL) 24
6.4.1 Safety Integrity Level in the Risk Graph Approach 25
6.4.2 Safety Integrity Level in the Probabilistic Approach 25
6.4.3 Safety Integrity Level 0 25

6.5 About part 1 of the standard 25

6.6 About part 2 of the standard 26

6.7 About part 3 of the standard 27

6.8 About the other parts of the standard 28

6.9 Abbreviations 29

7 APPENDIX 30

7.1 List of Documents 30

7.2 List of Activities 33

Figures

Figure 1: RiskCAT 61508 screen 3
Figure 2: RiskCAT screen parts 6
Figure 3: Presentation of the standard clauses in four levels 8

Acknowledgements and trademarks

All trademarks used in this manual are acknowledged.

Windows 9*, NT, 2000 and XP are trademarks of Microsoft

PDF is a trademark of Adobe Corporation USA

XpdfViewer is a trademark of Glyph & Cog.

InstallShield is a trademark of Macrovision Corporation.

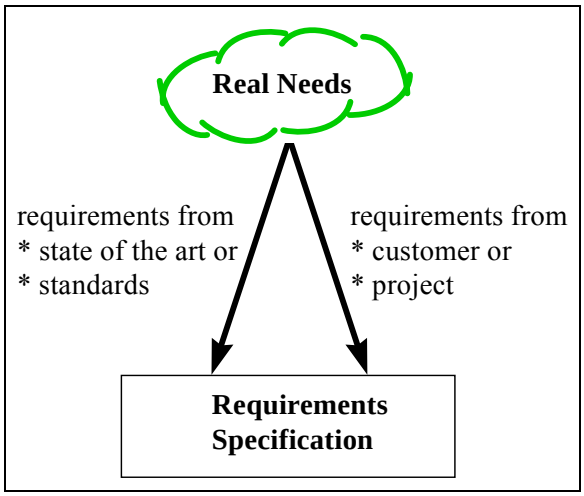
CATS Software Tools GmbH would like to thank our UK distributor PhaedruS Systems Ltd for proof reading & editing the English version of this manual. www.phaedsys.org

CATS Software Tools GmbH thanks the DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE and the IEC International Electrotechnical Commission for permission to reproduce extracts from International Standard IEC 61508.

All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on DKE is available from www.dke.de and on the IEC is available from www.iec.ch. DKE and IEC have no responsibility for the placement and context in which the extracts and contents are reproduced by CATS Software Tools GmbH; nor are DKE/IEC in any way responsible for the other content or accuracy therein.

1 Overview

Prerequisite to produce and certify high quality embedded systems including their software is to know about the functional and non functional requirements imposed on the embedded system. These requirements generally result from two different sources. One source is the specific requirements of the customer or producer e.g. based on their applications or marketing strategy. The other sources are the requirements imposed on the embedded system and its software by the state of the art represented e.g. by national or international standards.



RiskCAT is a tool of Code Analyzer Tool Set (CATS) for requirements capturing from standards thereby providing the starting point for high quality development and products in the area of embedded systems and their software. The state of the art in quality of EEPES (electrical / electronic / programmable electronic systems) is provided to a large extent by IEC 61508.

The design of RiskCAT is modular and widely configurable. It is possible (for CATS) to adopt the tool to modifications and enhancements of the standards applied as well as the extension to additional standards or other technical rules.

The work tasks assisted by RiskCAT 61508 are:

1. the selection of risk parameters,
2. the evaluation of risk classes based on the risk parameters selected,
3. manual pre-selection of risk class,
4. the structured overview on the recommended measures,
5. the selection of individual measures,
6. the selection of groups of measures according to the degree of obligation,
7. the selection of measures related to documents[1],
8. the selection of measures related to activities (life cycle phases)[2],
9. the selection of measures related to key words,
10. the copy function for actually marked measure into the clipboard,
11. the possibility to edit notes for each individual measure
12. overview on defined terms in the measures texts

[1] The set of documents used is based on Tables A.1 to A.3 of IEC 61508, Part 1

[2] The set of life cycle phases used is based on Tables A.1 to A.3 of IEC 61508, Part 1

13. retrieval in the original standards (available only if user has installed pdf files of the concerned standard in the RiskCAT target installation directory),
14. the context related presentation of the original standards clause,
15. the context related presentation of explanations to the clause given in IEC 61508 itself (available only for part of the clauses and only with the "RiskCAT Normal Version")
16. the context related presentation of terms used in the measure texts given in IEC 61508, part 4 (available only with the "RiskCAT Normal Version")
17. the storage of measure profiles as project or company templates in a project file (project storage),
18. the reloading of measure profiles
19. the result storage as text file (Rich Text Format, RTF) consisting of
    - selected risk parameters,
    - risk class,
    - selected measures and
    - the notes related to the selected measures

An important advantage of the tool supported approach is the possibility to vary interactively risk parameters, risk classes and sets of process and realization measures defining alternative or optimized sets of measures to reach specified quality, safety or reliability targets.

The purpose of RiskCAT 61508 is to assist the user in application of the IEC 61508. However, it is of course not the purpose of the tool to replace the standard. Anyhow the detailed and precise wording of the standards clauses needs to be considered to claim conformance with the standards. RiskCAT's condensed presentation of the standards contents has been established for the purpose of ease of work, overview and general navigation.

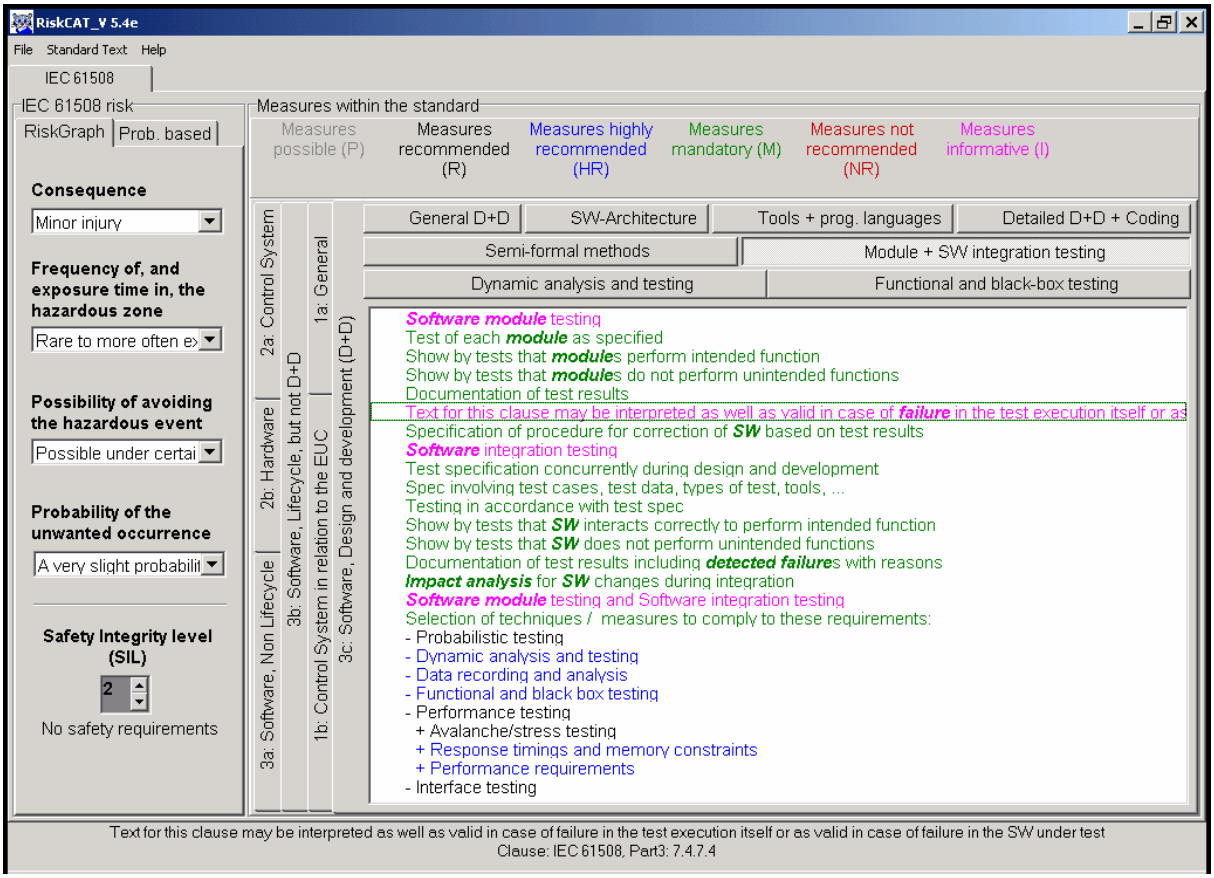

RiskCAT_V 5.4e
File Standard Text Help
IEC 61508
IEC 61508 risk
RiskGraph Prob. based
Consequence
Minor injury
Frequency of, and exposure time in, the hazardous zone
Rare to more often ex
Possibility of avoiding the hazardous event
Possible under certai
Probability of the unwanted occurrence
A very slight probabilit
Safety Integrity level (SIL)
2
No safety requirements
Measures within the standard
Measures possible (P)
Measures recommended (R)
Measures highly recommended (HR)
Measures mandatory (M)
Measures not recommended (NR)
Measures informative (I)
General D+D
SW-Architecture
Tools + prog. languages
Detailed D+D + Coding
Semi-formal methods
Module + SW integration testing
Dynamic analysis and testing
Functional and black-box testing
2a: Control System
1a: General
2b: Hardware
3b: Software, Lifecycle, but not D+D
1b: Control System in relation to the EUC
3a: Software, Non Lifecycle
3c: Software, Design and development (D+D)
Software module testing
Test of each module as specified
Show by tests that modules perform intended function
Show by tests that modules do not perform unintended functions
Documentation of test results
Text for this clause may be interpreted as well as valid in case of failure in the test execution itself or as
Specification of procedure for correction of SW based on test results
Software integration testing
Test specification concurrently during design and development
Spec involving test cases, test data, types of test, tools, ...
Testing in accordance with test spec
Show by tests that SW interacts correctly to perform intended function
Show by tests that SW does not perform unintended functions
Documentation of test results including detected failures with reasons
Impact analysis for SW changes during integration
Software module testing and Software integration testing
Selection of techniques / measures to comply to these requirements:
- Probabilistic testing
- Dynamic analysis and testing
- Data recording and analysis
- Functional and black box testing
- Performance testing
+ Avalanche/stress testing
+ Response timings and memory constraints
+ Performance requirements
- Interface testing
Text for this clause may be interpreted as well as valid in case of failure in the test execution itself or as valid in case of failure in the SW under test
Clause: IEC 61508, Part3: 7.4.7.4

Figure 1: RiskCAT 61508 screen

RiskCAT is designed for use by embedded systems software professionals. Experience of using Windows on PCs is required.

2 Installation / First Start / Deinstallation

2.1 The components of RiskCAT

RiskCAT is an application for Windows 2000/ NT/ XP®. It is distributed on an **USB memory stick**.

The **USB memory stick** has the following directory structure:

- RiskCAT_61508 with the subdirectory
  - XPDF
- Tool_Documentation
- CATS_Information

The directory RiskCAT_61508 contains besides other files:

- The RiskCAT executable **RiskCAT_61508_V54e.exe**.
- The help file **RiskCAT_61508_V54e.hlp**.
- The help content file **RiskCAT_61508_V54e.cnt.**
- The standard files **IEC61508_*_GB_1.pdf**.

The subdirectory XPDF of directory RiskCAT_61508 contains:

- The XpdfViewer™ ActiveX Control, Version 3.0, **XpdfViewerCtrl.ocx**.

The sub-subdirectory t1fonts in the subdirectory XPDF contains

- the fonts needed by the XpdfViewer

The directory Tool_Documentation contains:

- The product description **RiskCAT_61508_V5_Product_4.pdf**
- This user manual **RiskCAT_61508_UserManual_54e.pdf**

The directory CATS_Information contains:

- The product description **RiskCAT_50128_V411_Product.pdf**
- The description of the Static Analyzers of the Code Analyzer Tool Set, Overview and Motivation, **StaticAnalyzers_5.pdf**.

Because of licensing conditions the standard files

- IEC61508_*_GB_1.pdf

are for use with RiskCAT only.

2.2 Local Operation on a PC

RiskCAT 61508 does not need any installation. Just run the executable file RiskCAT_61508_V54e.exe from the directory RiskCAT 61508 on the USB memory stick.

CAUTION: The execution of **RiskCAT_61508_V54e** is possible only from the original USB memory stick. For backup purpose the stick contents may be copied to any backup device. However, RiskCAT_61508_V54e will operate from the memory stick only.

CAUTION: The first execution of **RiskCAT_61508_V54e** will install the XpdfViewer™ ActiveX Control, Version 3.0, on the local PC. In case of version conflicts with a XpdfViewer already installed please contact CATS via info@cats-tools.de.

2.3 Uninstallation on a local PC

As RiskCAT 61508 does not need any installation so it does neither need any uninstallation.

Uninstallation of XpdfViewer is accomplished by running WINDOWS-System-Control > Software > Installation/Uninstallation > selecting the XpdfViewer control.

2.4 Network Installation of RiskCAT

RiskCAT offers two different possibilities for network installations:

- You may access RiskCAT_61508_V54e on the USB memory stick network wide or
- you may use a disk drive based installation.

For both types of network installation a single RiskCAT executable is relocated on the server USB / disk drive. Additionally one XPDF Viewer is installed on each client (automatically installation by RiskCAT in the start-up phase).

CAUTION: The number of simultaneous usage is limited by the licensed number of users.

Please contact us for further information via info@cats-tools.de.

3 Basics

3.1 Screen parts

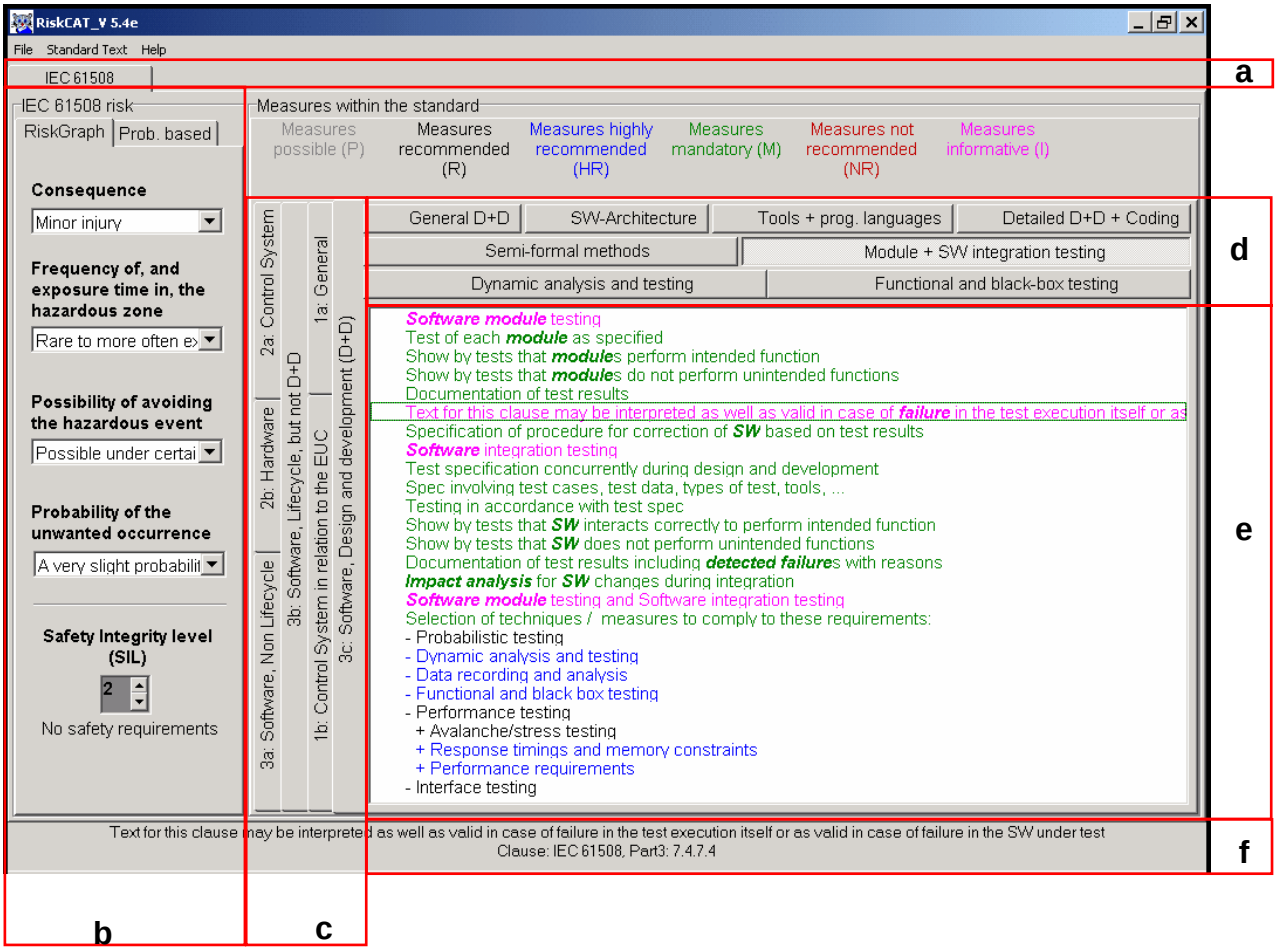

RiskCAT_V 5.4e
File Standard Text Help
IEC 61508
a
IEC 61508 risk
RiskGraph Prob. based
Consequence
Minor injury
Frequency of, and exposure time in, the hazardous zone
Rare to more often e
Possibility of avoiding the hazardous event
Possible under certai
Probability of the unwanted occurrence
A very slight probabilit
Safety Integrity level (SIL)
2
No safety requirements
b
Measures within the standard
Measures possible (P)
Measures recommended (R)
Measures highly recommended (HR)
Measures mandatory (M)
Measures not recommended (NR)
Measures informative (I)
2a: Control System
2b: Hardware
3a: Software, Non Lifecycle
3b: Software, Lifecycle, but not D+D
1b: Control System in relation to the EUC
1a: General
3c: Software, Design and development (D+D)
c
General D+D
SW-Architecture
Tools + prog. languages
Detailed D+D + Coding
Semi-formal methods
Module + SW integration testing
Dynamic analysis and testing
Functional and black-box testing
d
Software module testing
Test of each module as specified
Show by tests that modules perform intended function
Show by tests that modules do not perform unintended functions
Documentation of test results
Text for this clause may be interpreted as well as valid in case of failure in the test execution itself or as
Specification of procedure for correction of SW based on test results
Software integration testing
Test specification concurrently during design and development
Spec involving test cases, test data, types of test, tools, ...
Testing in accordance with test spec
Show by tests that SW interacts correctly to perform intended function
Show by tests that SW does not perform unintended functions
Documentation of test results including detected failures with reasons
Impact analysis for SW changes during integration
Software module testing and Software integration testing
Selection of techniques / measures to comply to these requirements:
- Probabilistic testing
- Dynamic analysis and testing
- Data recording and analysis
- Functional and black box testing
- Performance testing
+ Avalanche/stress testing
+ Response timings and memory constraints
+ Performance requirements
- Interface testing
e
Text for this clause may be interpreted as well as valid in case of failure in the test execution itself or as valid in case of failure in the SW under test
Clause: IEC 61508, Part3: 7.4.7.4
f

Figure 2: RiskCAT screen parts

a: Standard tabs

b: Risk window

c: Area tabs

d: Topic tabs

e: Measure window

f: Information line

3.2 Interrelationship between the screen parts

The screen parts c, d and e are used to present the measures.

The Safety Integrity Level (SIL) selected in screen part b controls the degree of obligation of the measures given in screen part e.

However, the two screen parts are largely independent from each other. The screen relationship between the measures group (parts c, d & e) and the SIL block on the left may be adjusted. This is accomplished by a single left mouse button click on the boarder line between the screen parts b and c and moving the mouse afterwards

CAUTION: The measures selected in screen part e are consistent with the safety integrity level shown in screen part b only if the RiskCAT usage is according to chapter 4.6, "Selection of groups of measures according to the degree of obligation", of this manual.

3.3 Measure states

RiskCAT applies a three dimensional state to each measure. The three state dimensions are

- marked / unmarked
- selected / deselected
- with comment / without comment

The state "marked" may be assigned to one measure only at any time. Marking of a measure is by a single left mouse button click. It is visible by a box around the text describing the measure.

The state "selected" may be assigned to one, several or even all measures at the same time. Manual election of a measure is by a single left mouse button click. It is visible by a tick ✓ left of the text describing the measure. Automatic selection is discussed later in this manual (see chapters 4.6, "Selection of groups of measures according to the degree of obligation", to 4.9, "Selection of measures related to key words").

The state "with comment" may be assigned to one, several or even all measures at the same time. Adding comments to a measure is via context menu (depress of right mouse button) in the measure list boxes. It is visible by a left of the text describing the measure.

3.4 Measure colours

The measures in screen part "e" are dynamically coloured depending on their level, Possible (grey), Recommended (black), Highly recommended (red), Mandatory (green), NOT recommended (red) and informative (pink) as indicated by the SIL selected in screen area "b".

CAUTION: The screen shown in Figure 2 has all levels, Recommended, Highly recommended, Mandatory, NOT recommended and informative. All users who may be

colour blind should go to "7. Software, Design and development (D+D)" and Tab "SW-Architecture" and set the SIL to 3. Then select in turn each of the measure settings to get the check mark ✓ by the relevant measures.

3.5 Structure of the measures presentation used with RiskCAT

RiskCAT starts from standards. So the original sets of measures are the **standards** represented by the standard tabs (marked with "a" in Figure 2).

A standard may consist of different parts as e.g. IEC 61508 has 7 parts. The standard or even its parts may be such voluminous that it is not appropriate to use all measures as an entity. This has been the reason to break down some standards into **areas** represented by the area tabs (marked with "c" in Figure 2). Depending on the standard an area may consist of a part of a standard, some clauses of a standard or some clauses of a part of a standard. For details see the standard specific descriptions in this manual.

Most standards cover a variety of **topics** represented by the topic tabs (marked with "d" in Figure 2). The approach has been to have an assignment between standards chapters and RiskCAT topics. However, in some cases standard chapters have been further split up, because of a high number of measures or because of different matters covered in the same chapter.

A further structuring is by grey shaded areas in the measure window. This presentation indicates that the marked requirements are alternatives to each other.

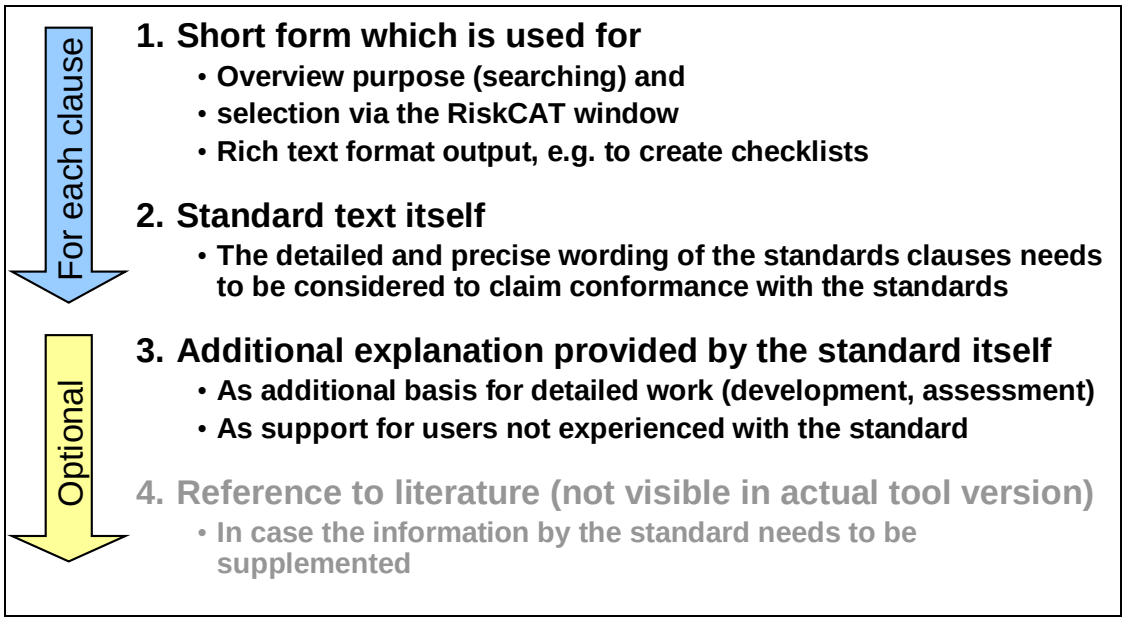
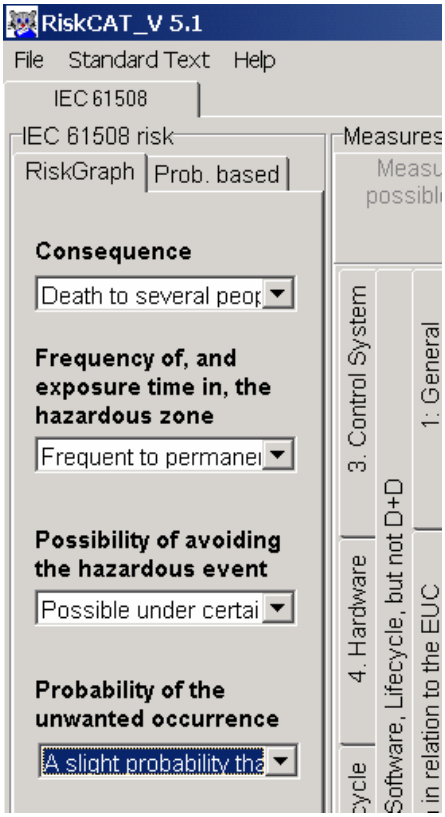

For each clause
Optional
1. Short form which is used for
• Overview purpose (searching) and
• selection via the RiskCAT window
• Rich text format output, e.g. to create checklists
2. Standard text itself
• The detailed and precise wording of the standards clauses needs to be considered to claim conformance with the standards
3. Additional explanation provided by the standard itself
• As additional basis for detailed work (development, assessment)
• As support for users not experienced with the standard
4. Reference to literature (not visible in actual tool version)
• In case the information by the standard needs to be supplemented

Figure 3: Presentation of the standard clauses in four levels

4 Tasks

4.1 Selection of risk parameters



Defining risk parameters is performed in the risk window. First step is the selection of the approach by the approach tabs

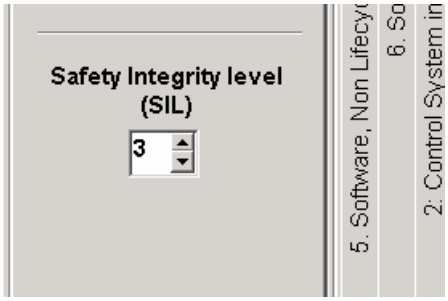
- RiskGraph, or
- Prob.based (Probability based).

Second step is selecting the risk parameter from the approach specific selection boxes.

For details of the IEC 61508 risk parameter selection see chapter 6.4, "About the Safety Integrity Level (SIL)" of this manual.

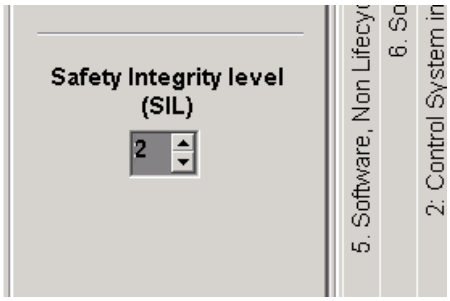
In the selection "RiskGraph" full text of risk parameters is presented in the RiskCAT Information line at bottom line of screen (screen part "f" in Figure 2).

4.2 Evaluation of Safety Integrity Level based on the risk parameters selected



The Safety Integrity Level is automatically processed by change of any influencing risk parameter. It is displayed at the bottom of risk window.

4.3 Manual pre selection of the Safety Integrity Level

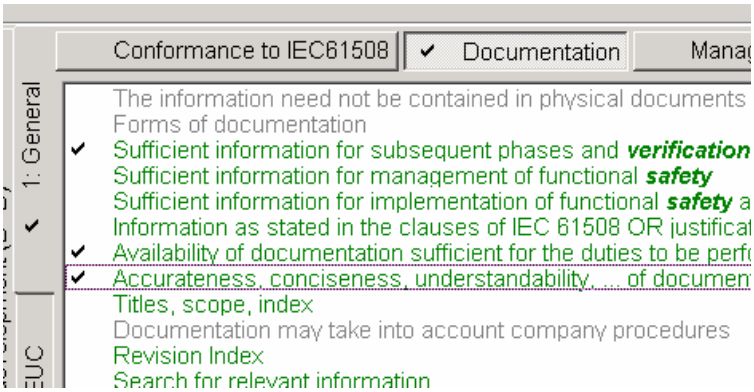


The Safety Integrity Level applied to the measures can be modified directly and independently from risk parameter selection by using the up/down switches of Safety Integrity Level control. In this case the Safety Integrity Level background is greyed to indicate there is a mismatch between the SIL used and the risk parameters selected.

4.4 Structured overview on the recommended measures

Each of the area tabs represents an important theme within the scope of embedded controllers and their software. And each of the topic tabs represents a coherent set of measures. Just by selection of corresponding tabs RiskCAT provides an overview about the measures with respect to the topic given as tab text.

4.5 Selection of individual measures

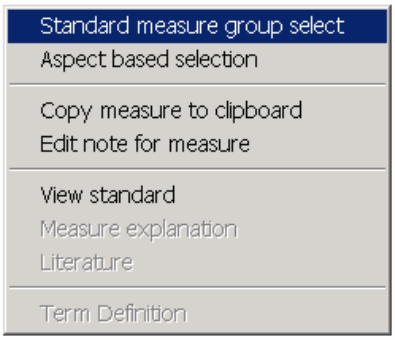

Conformance to IEC61508
Documentation
1: General
The information need not be contained in physical documents
Forms of documentation
Sufficient information for subsequent phases and verification
Sufficient information for management of functional safety
Sufficient information for implementation of functional safety a
Information as stated in the clauses of IEC 61508 OR justificat
Availability of documentation sufficient for the duties to be perf
Accurateness, conciseness, understandability, ... of documen
Titles, scope, index
Documentation may take into account company procedures
Revision Index
Search for relevant information

Individual measures are selected / deselected by a double click with left mouse button. Selection is visible by

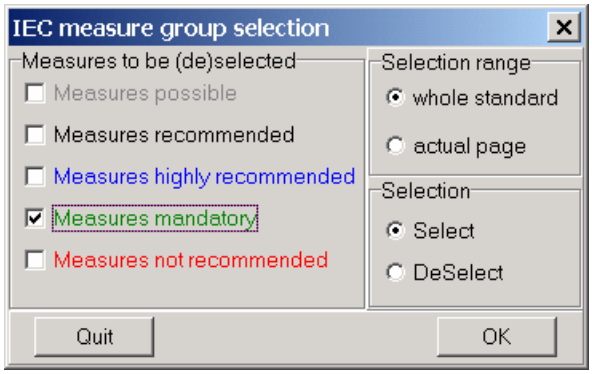
- A check mark ✓ to the left of the measure itself
- A check mark ✓ to the left of the corresponding topic tab
- a check mark ✓ to the left of the corresponding area tab

The selection is in addition to already selected measures. If the real interest is just to concentrate on the measures actually selected; precautions need to be applied to de-select any measures that may have been selected previously. See next chapter of this manual for global selection/ de-selection of measures.

4.6 Selection of groups of measures according to the degree of obligation



The selection of groups according to the degree of obligation3, under the currently selected SIL, of the measures is activated via context menu (depress of right mouse button) in the measure window (screen part "e" in Figure 2).



After choice of "Standard measure group selection" the selection form shown on the left appears.

If the "whole standard" is activated the selection will be for all measures in all areas for all topics.

If the "actual page" is activated the selection will be just for the measures in visible topic tab.

The visibility of the selection is same as for individual measures selection.

CAUTION: If you change the SIL between group selection and the "DeSelect" the set of deselected measures may be different from the selected set. So here "DeSelect" is only the inverse function to "Select" if SIL is the same for both actions.

The selection is in addition to already selected measures. If the real interest is just to concentrate on the measures you are about to select then precautions need to be applied that at on starting measure selection no measures are already selected.

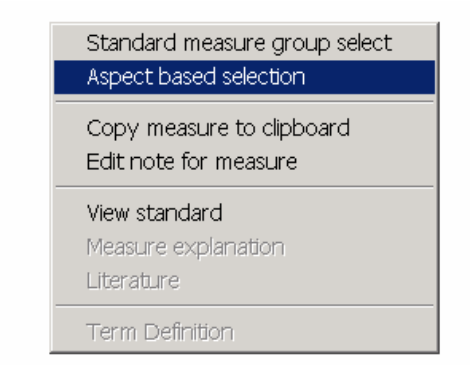
Example for the usage of selection of groups of measures:

IEC 61508 in certain places explicitly mentions that certain solutions are "possible". Key word in the standard is "may".

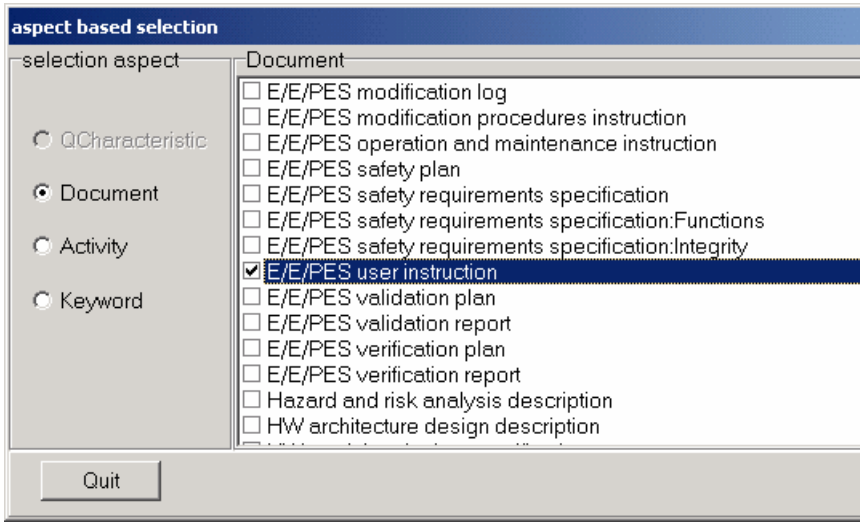
If you doubt whether you may allocate a safety function across more than one safety-related system you should select all possible measures and check them afterwards.

[3] For the degree of obligation please refer as well to chapter 6.1, "Presentation of the degree of obligation of the requirements".

4.7 Selection of measures related to documents



The document related selection functionality is activated via context menu (depress of right mouse button) in the measure window (screen part "e" in Figure 2).



After choice of "Aspect based selection" the selection form shown on the left appears.

The set of documents is based on Tables A.1 to A.3 of IEC 61508, Part 1. It is listed in Appendix 7.1 "List of Documents", page 30, of this manual.

Apart from the possibility to select according to the documents list RiskCAT offers selection according to activity (life cycle phase). Of course "documents" and "life cycle phases" are related to each other. However, in IEC 61508 a phase generally results in several documents and on the other hand a document may be used for different phases. Therefore RiskCAT uses documents as well as activities.

If you are interested in a very specific selection you should just apply a single document or activity.

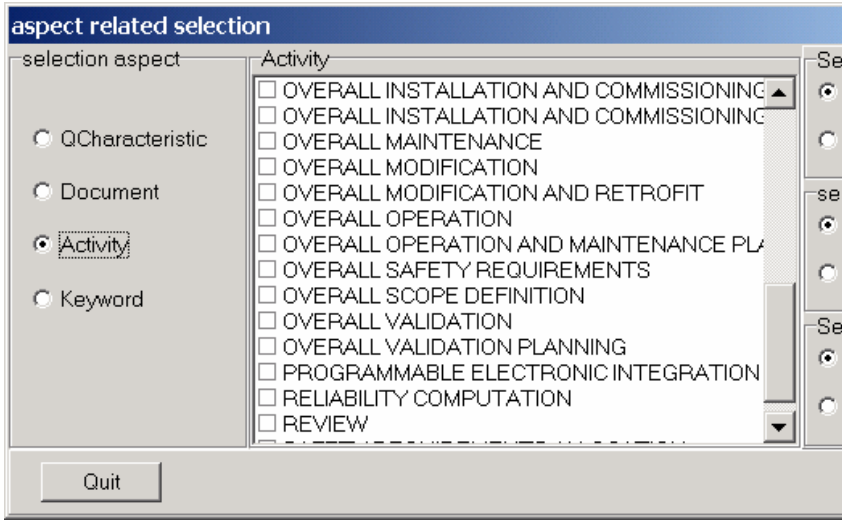
If your interest is to get a complete view you should run two selections after each other:

- In one "or type" selection choose the *document* of your specific interest as well as "All". Terminate it with "Ok".
- In the other "or type" selection choose the *activity* related to the document of your specific interest as well as "All". Terminate it again with "Ok".

The selection is in addition to already selected measures. So precautions need to be applied that at starting no measures are selected.

4.8 Selection of measures related to activities (life cycle phases)

As the with the "document" related selection functionality the "activity" related selection is activated via context menu (depress of right mouse button) in the measure window (screen part "e" in Figure 2).



After choice of "Aspect based selection" the selection form shown on the left appears.

The set of activities is based on Tables A.1 to A.3 of IEC 61508, Part 1. It is listed in Appendix 7.2, "List of Activities", page 33, of this manual.

The selection is in addition to already selected measures. So precautions need to be applied that at starting no measures are selected.

4.9 Selection of measures related to key words

The "Keyword" related selection functionality is activated via context menu (depress of right mouse button) in the measure window (screen part "e" in Figure 2).

The set of keywords has been created based on work with and discussion about IEC 61508 by the authors.

The selection is in addition to already selected measures. So precautions need to be applied that at starting no measures are selected.

4.10 Copying the actually marked measure into the clipboard

The copy to clipboard functionality is activated via context menu in the measure window (screen part "e" in Figure 2).

The steps are:

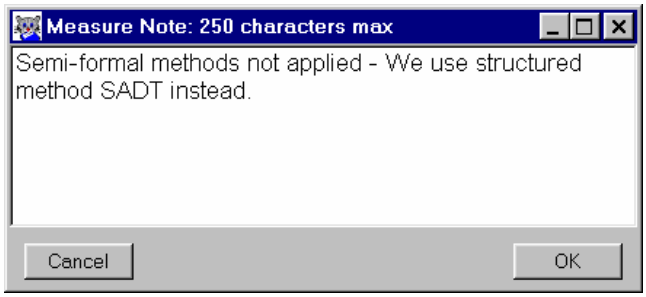
- Mark the measure to be copied by a single left mouse button click. (Otherwise no measure will be found on the clipboard later on.)
- Activate context menu (depress right mouse button while the pointer is in the measure window)
- Choose "Copy selected measure to clipboard" to copy contents of the state line
- Use an application with clipboard functionality
- Insert or paste clipboard contents

4.11 Edit notes to the marked measure

Purpose of edit notes is to provide:

- Space for comments on a specific project, e.g. to log the reasoning for not selecting particular measures for the project
- Company specific frames of prescribed measures as well as company specific interpretations of measures
- Log results from audits, reviews, or tests.

The edit measure note functionality is activated via context menu in the measure window.



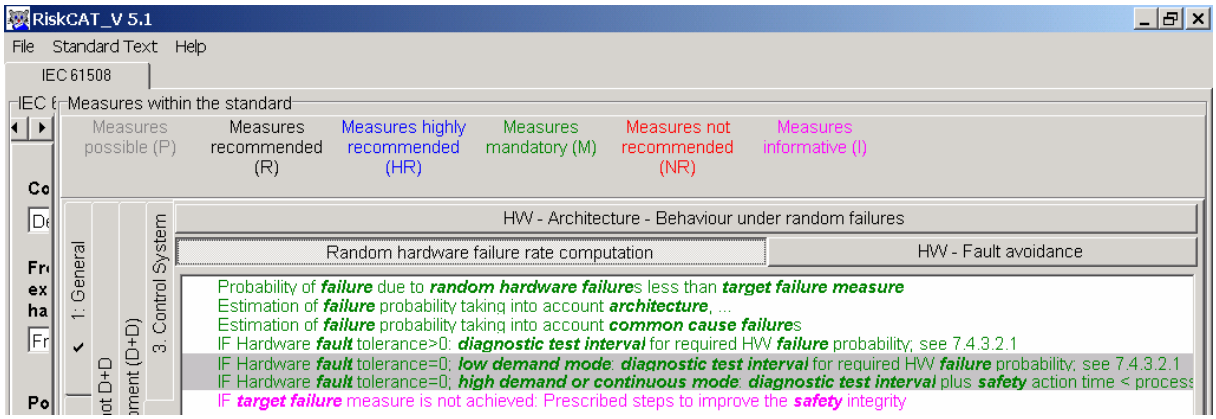
The steps are:

- Mark the measure for which the item note shall be edited by a single left mouse button click. Otherwise nothing visible to the user will occur.
- Activate context menu. Depress right mouse button while the pointer is in the measure window (screen part "e" in Figure 2).
- choose „Edit note for measure"

For looking to existing notes or modifying them choose "Edit note for measure" again. Notes are saved via Project storage (see chapter 4.17, "Project (session) storage in a file" of this manual). They may be reloaded by Project reload.

4.12 Overview on defined terms in the measures texts

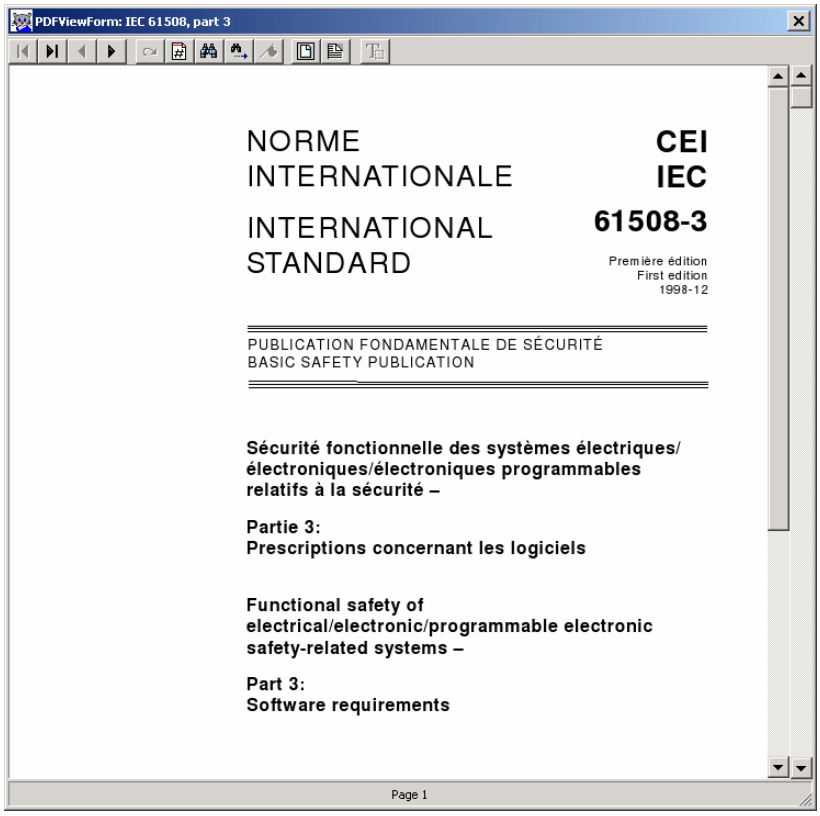
As shown in the figure below terms defined in IEC 61508, part 4, are highlighted in **bold type** in the presentation of the measure texts.


RiskCAT_V 5.1
File
Standard Text
Help
IEC 61508
Measures within the standard
Measures possible (P)
Measures recommended (R)
Measures highly recommended (HR)
Measures mandatory (M)
Measures not recommended (NR)
Measures informative (I)
HW - Architecture - Behaviour under random failures
Random hardware failure rate computation
HW - Fault avoidance
1: General
3. Control System
Probability of failure due to random hardware failures less than target failure measure
Estimation of failure probability taking into account architecture, ...
Estimation of failure probability taking into account common cause failures
IF Hardware fault tolerance>0: diagnostic test interval for required HW failure probability; see 7.4.3.2.1
IF Hardware fault tolerance=0; low demand mode: diagnostic test interval for required HW failure probability; see 7.4.3.2.1
IF Hardware fault tolerance=0; high demand or continuous mode: diagnostic test interval plus safety action time < process
IF target failure measure is not achieved: Prescribed steps to improve the safety integrity

Just scrolling through the measures provides an overview about the defined terms used in the measures texts.

4.13 Retrieval in the original standards

RiskCAT offers an interface for viewing the original standards. For this the XpdfViewer™ XpdfViewerCtrl.ocx library is implemented.



Prerequisite for the retrieval is the availability of licensed standard files. With the Basic Package IEC 61508 parts 1, 2 and 3 are available. And with the Normal Package parts 4 and 7 are also provided.

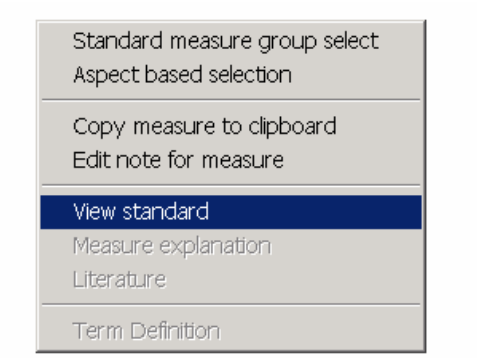
Retrieval is started via "Standard Text" menu. The size of the standards window may be changed by positioning the mouse on the windows border (preferred on the left or right hand side) followed by pressing the left mouse button and then moving it.

The XpdfViewer™ provides the following functions:

- First page
- Last page
- Previous page
- Next page
- Back to selection
- Go to page
- Find
- Find next
- Add page to hotlist
- Adjust to page height
- Adjust to page width
- Copy text to clipboard

4.14 Context related retrieval in the original standards

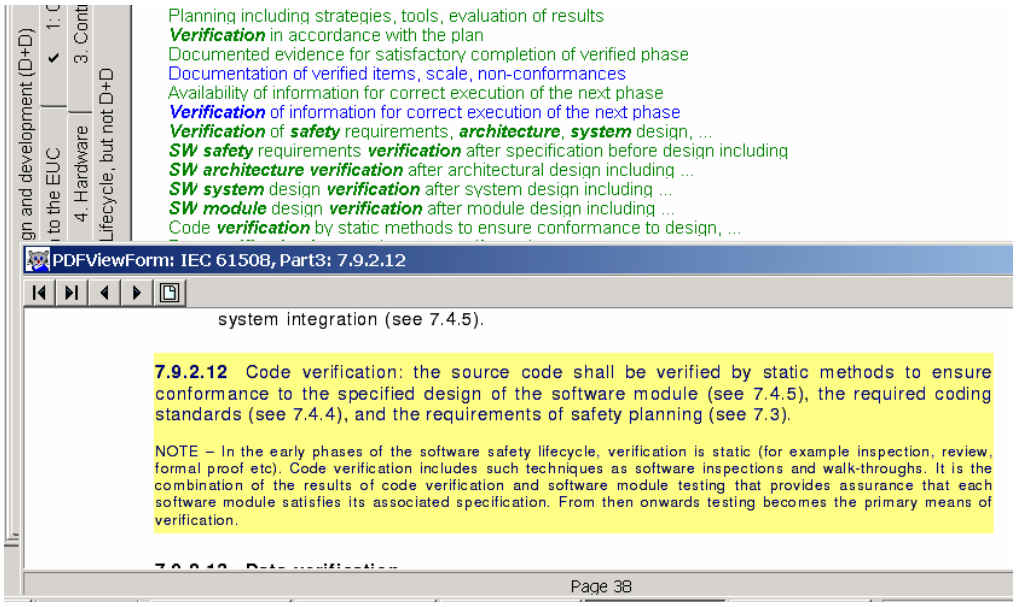
Besides the interface for full text browsing RiskCAT offers an interface for context sensitive browsing in original standards. Again prerequisite for this task is the availability of licensed standard files. With the Basic Package IEC 61508 parts 1, 2 and 3 are available. And with the Normal Package parts 4 and 7 are also provided.



The context related retrieval is activated via context menu in the measure window (screen part "e" in Figure 2). The steps are:

- Mark the measure establishing the context by a single left mouse button click. (Otherwise the page selected by context related retrieval is somewhat arbitrary.)
- Activate context menu (depress right mouse button while the pointer is in the measure window)
- Choose "View standard"

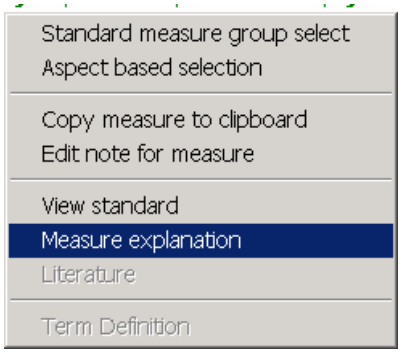
RiskCAT will show the page of the standard highlighting the clause in context. The size of the standards window may be changed by positioning the mouse on the windows border (preferred on the left or right hand side) followed by pressing the left mouse button and then moving it


Planning including strategies, tools, evaluation of results
Verification in accordance with the plan
Documented evidence for satisfactory completion of verified phase
Documentation of verified items, scale, non-conformances
Availability of information for correct execution of the next phase
Verification of information for correct execution of the next phase
Verification of safety requirements, architecture, system design, ...
SW safety requirements verification after specification before design including
SW architecture verification after architectural design including ...
SW system design verification after system design including ...
SW module design verification after module design including ...
Code verification by static methods to ensure conformance to design, ...
PDFViewForm: IEC 61508, Part3: 7.9.2.12
system integration (see 7.4.5).
7.9.2.12 Code verification: the source code shall be verified by static methods to ensure conformance to the specified design of the software module (see 7.4.5), the required coding standards (see 7.4.4), and the requirements of safety planning (see 7.3).
NOTE – In the early phases of the software safety lifecycle, verification is static (for example inspection, review, formal proof etc). Code verification includes such techniques as software inspections and walk-throughs. It is the combination of the results of code verification and software module testing that provides assurance that each software module satisfies its associated specification. From then onwards testing becomes the primary means of verification.
Page 38

If other PDF versions of the standards have been installed than those supplied by CATS RiskCAT may show the wrong page and may highlight the wrong clause. Therefore only those standards supplied by CATS should be used with the RiskCAT tools.

4.15 The context related presentation of explanations to the clause provided by IEC 61508 itself

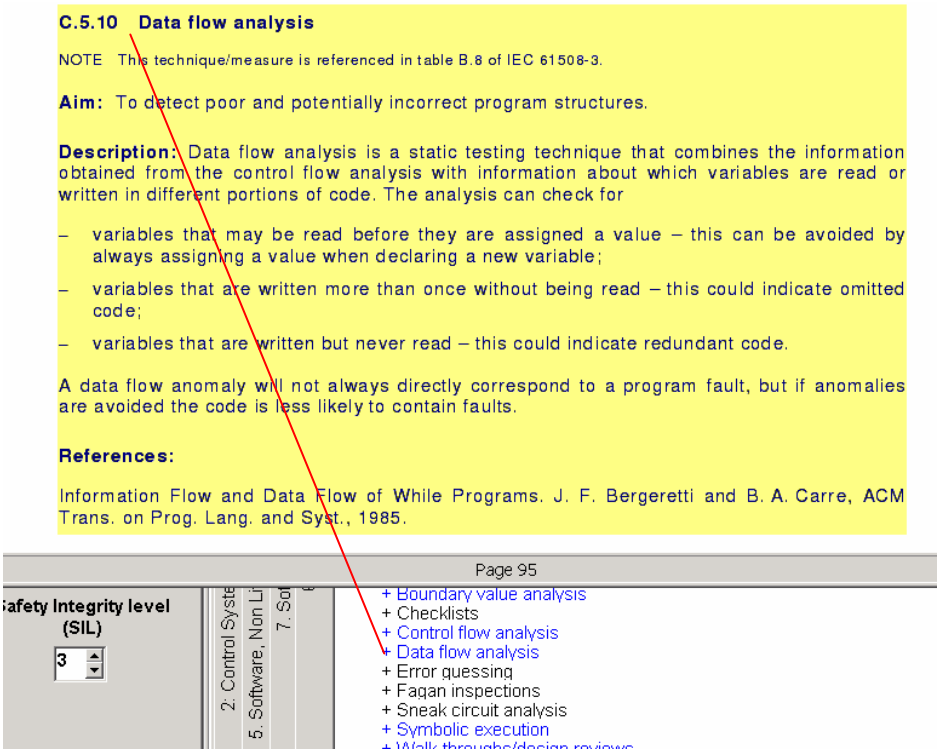
For certain clauses IEC 61508 itself provides additional explanations, mostly from part 7 of the standard. RiskCAT offers an interface for context sensitive browsing the explanations from the original standard. However, only the RiskCAT Normal package offers access to part 7.



The context related explanation is activated via context menu in the measure window. The steps are:

- Mark the measure establishing the context by a single left mouse button click. (Otherwise the page selected by context related retrieval is somewhat arbitrary.)
- Activate context menu (depress right mouse button while the pointer is in the measure window)
- Choose "Measure explanation"

RiskCAT will show the page of the standard highlighting the explanation in context. The size of the standards window may be changed by positioning the mouse on the windows border (preferred on the left or right hand side) followed by pressing the left mouse button and then moving it.

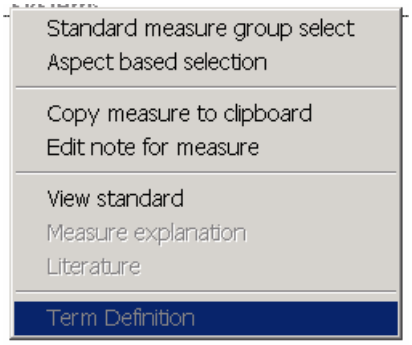

C.5.10 Data flow analysis
NOTE This technique/measure is referenced in table B.8 of IEC 61508-3.
Aim: To detect poor and potentially incorrect program structures.
Description: Data flow analysis is a static testing technique that combines the information obtained from the control flow analysis with information about which variables are read or written in different portions of code. The analysis can check for
– variables that may be read before they are assigned a value – this can be avoided by always assigning a value when declaring a new variable;
– variables that are written more than once without being read – this could indicate omitted code;
– variables that are written but never read – this could indicate redundant code.
A data flow anomaly will not always directly correspond to a program fault, but if anomalies are avoided the code is less likely to contain faults.
References:
Information Flow and Data Flow of While Programs. J. F. Bergeretti and B. A. Carre, ACM Trans. on Prog. Lang. and Syst., 1985.
Page 95
afety Integrity level (SIL)
3
2. Control Syste
5. Software, Non Li
7. So
+ Boundary value analysis
+ Checklists
+ Control flow analysis
+ Data flow analysis
+ Error guessing
+ Fagan inspections
+ Sneak circuit analysis
+ Symbolic execution

If other PDF versions of the standards have been installed than those supplied by CATS RiskCAT may show the wrong page and may highlight the wrong clause. Therefore only those standards supplied by CATS should be used with the RiskCAT tools

4.16 The context related presentation of terms used in the measure texts given in IEC 61508, part 4

For certain terms IEC 61508 part 4 provides definitions. The RiskCAT Normal Package offers an interface for context sensitive browsing the definitions from the original standard.

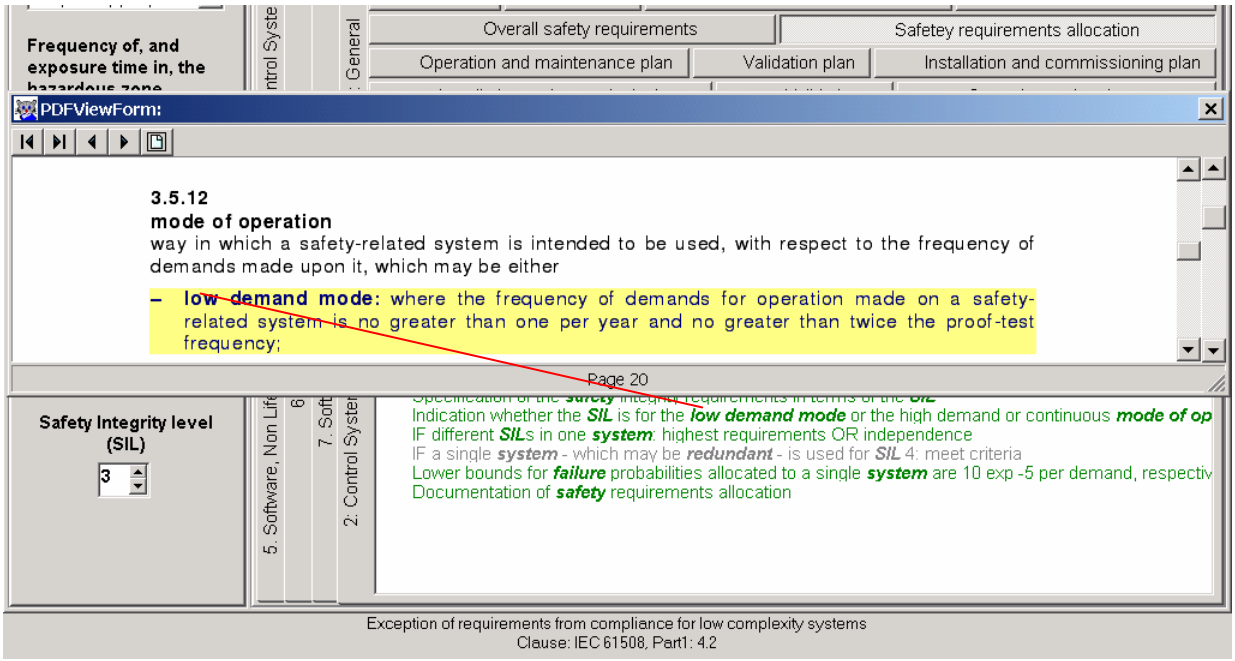
The defined terms used in the measures presentation are presented in bold.



The context related term definition is activated via context menu in the measure window. The steps are:

- Go with the cursor to a defined (**bold**) term. The type of the cursor which normally is ↖ then will change to ☝
- Activate context menu (depress right mouse button while the pointer is in the measure window)
- Choose "Term Definition"

RiskCAT will show the page of the standard highlighting the definition in context. The size of the standards window may be changed by positioning the mouse on the windows border (preferred on the left or right hand side) followed by pressing the left mouse button and then moving it.


Frequency of, and exposure time in, the
Overall safety requirements
Safetey requirements allocation
Operation and maintenance plan
Validation plan
Installation and commissioning plan
PDFViewForm:
3.5.12
mode of operation
way in which a safety-related system is intended to be used, with respect to the frequency of demands made upon it, which may be either
– low demand mode: where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof-test frequency;
Page 20
Safety Integrity level (SIL)
3
Indication whether the SIL is for the low demand mode or the high demand or continuous mode of op
IF different SILs in one system: highest requirements OR independence
IF a single system - which may be redundant - is used for SIL 4: meet criteria
Lower bounds for failure probabilities allocated to a single system are 10 exp -5 per demand, respectiv
Documentation of safety requirements allocation
Exception of requirements from compliance for low complexity systems
Clause: IEC 61508, Part1: 4.2

If other PDF versions of the standards have been installed than those supplied by CATS RiskCAT may show the wrong page and may highlight the wrong clause. Therefore only those standards supplied by CATS should be used with the RiskCAT tools.

4.17 Project (session) storage in a file

Project storage has two distinct purposes one for the 'normal' user and another for the project leader or the quality manager.

- For the *'normal' user* it offers the possibility to interrupt and resume RiskCAT tool sessions. For this purpose the actual status is stored in binary RiskCAT project files.
- For the *project leader* or the quality manager it offers the possibility to fill in the comments to the measures. Thereby advice may be given to the 'normal' user by which means (e.g. tools, procedures, forms) compliance with the measure shall be achieved in a specific project. If certain measures are not applicable in a specific project or for a specific part of a project background for this may be supplied as comment as well. So the comments result in a company or project specific framework. This framework - or requirements capture - may be stored and used as a starting point by the 'normal' users.

The storage function is chosen by item "Store project" in "File" menu.

4.18 Project (session) reload from a file

- For a new session the framework prepared by the project leader or the quality manager may be loaded.
- An interrupted and stored tool session may be resumed.

The restore function is chosen by item "Load project" in "File" menu.

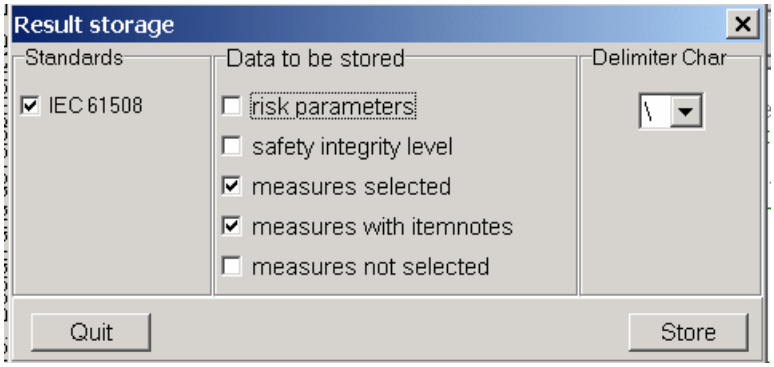
4.19 Result storage as RTF-file

For further documentation, e.g. creation of checklists or test plans, RiskCAT offers storage as text file (Rich Text Format, RTF) of:

- The selected risk parameter,
- The Safety Integrity Level (SIL) as shown in the risk window (that is either the SIL resulting from risk parameters or the manually pre selected one)
- Three sets of measures
  - Measures contained in more than one set are stored once only

For each measure following items are stored

- The measure text (text of the level 1 presentation),
- The reference to part as well as clause of IEC 61508,
- The degree of obligation,
- The note.



Result storage is started via the menu "File". For result storage there are some options given in the menu in a self-explaining manner. The option to select a delimiter character supports an import of the stored data in tables by a text processor.

IEC 61508 results

Safety Integrity Level: 2 Value is valid

Measure	***Reference in the part of IEC 61508***	***Degree of obligation for selected SIL*[4]**	**Note**
Clear, precise, verifiable, maintainable, ... specification	IEC 61508, Part2: 7.2.2.2	M	
Use of appropriate techniques to avoid mistakes during specification:	IEC 61508, Part2: 7.2.3.3	M	
- Structured specification	IEC 61508, Part2: 7.2.3.3 / Table B.1	HR	Company Standard: Structure of the Specification according to form "Spec" from Quality Management System
- Computer aided specification tools	IEC 61508, Part2: 7.2.3.3 / Table B.1	R	Company Standard: Use of CALIBER

[4] For the meaning of the abbreviations in this column please refer to chapter 6.1, "Presentation of the degree of obligation of the requirements"

5 Menu functions

5.1 "File" menu

Functions within file menu are:

- Result storage – see chapter 4.19, "Result storage as RTF-file"
- Caliber result storage – for future use
- Load project – see chapter 4.18, "Project (session) reload from a file"
- Store project – see chapter 4.17, "Project (session) storage in a file"
- Exit – closes RiskCAT.

5.2 "Standard Text" menu

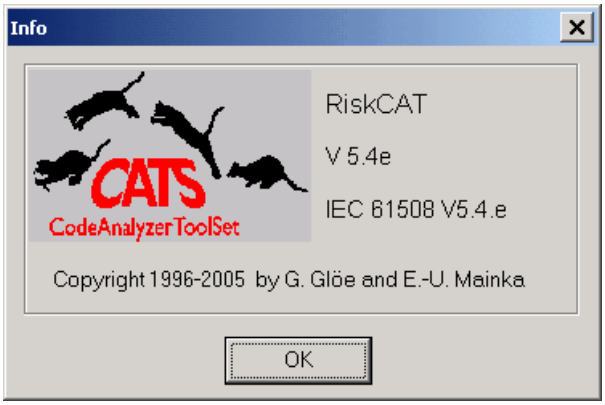
Functions within standards text menu are:

- Standard view by XpdfViewer™ – see chapter 4.13, "Retrieval in the original standards"

5.3 "Help" menu

Functions within help menu are:

- Help – Main texts of this user's manual are supplied as help.
- About – Informs about RiskCAT version and copyright



The upper line in the besides figure identifies the version of RiskCAT 61508 (V5.4e).

The lower line identifies the version of the database (IEC 61508 V5.2.e), which is included in RiskCAT.

6 IEC 61508 specific features

Importance of IEC 61508results from two objectives given in the scope of the standard:

- it is the basis for development of application sector international standards
- it is usable for applications without sector standards

To provide a good overall view on the measures required by IEC 61508 the main part requirements and the contents of tables have been integrated as far as reasonably possible. The number of tabs has been kept acceptable low by this.

6.1 Presentation of the degree of obligation of the requirements

Up to date IEC standards as IEC 61508 use four key words to identify their requirements (the first three explanations are from chapter 3, Definitions, of IEC 61226):

shall indicates requirements that are mandatory for compliance with the standard

should indicates requirements that are not mandatory for compliance with the standard but are strongly recommended

may indicates that compliance with the recommendation is optional

must not indicates requirements that are mandatory for compliance with the standard

Furthermore IEC 61508 indicates in tables specific requirements related to Safety Integrity Levels (SIL) as highly recommended, recommended, possible, or not recommended.

Within RiskCAT only one set of key words for the degree of obligation of requirements is used. To realize this

- shall requirements are classified as 'mandatory'
- should requirements are classified as 'highly recommended'
- may recommendations are classified as 'possible'
- must not requirements are classified as 'mandatory'

for all SILs.

Contents from notes and informative annexes have not been adopted to RiskCAT generally. However, in a very few cases it was felt that they are essential for application of the standard. As a consequence those are expressed explicitly in the tool.

Requirements from IEC 61508 related to production of further standards have not been implemented in RiskCAT.

6.2 About the license for the standards supplied with RiskCAT

By contract with the German Chapter of the IEC (DKE) CATS has been asked to declare with RiskCAT[5]:

> "The data from the international standards series IEC 61508 are in use with permission of the IEC International Electrotechnical Commission, Geneva. They have not been checked by IEC or their deputies.
>
> Authoritative for the application of the standard are the versions with newest edition which may be received from VDE VERLAG GMBH, Bismarckstr. 33, D-10625 Berlin (www.vde-verlag.de). The user shall pay attention to the national standards.
>
> CATS declares that texts used correspond to the actual state of the IEC-standards.
>
> 2001-09-24, CATS"

6.3 About some Key-Words in the individual measure presentation in RiskCAT

To a certain extent IEC 61508 clauses themselves give a condition for their applicability. To ease identification of these conditionally applicable clauses RiskCAT presents the respective individual measures starting with the Key-Word "***IF***". The end of the condition is denoted by "**:**".

Some clauses "do not apply in the case of" a certain condition (e.g. clause 7.4.5 of part 2). This is presented by RiskCAT by the Key-Word "***IF NOT***". Again the end of the condition is denoted by "***:***".

To a certain extent again within a single IEC 61508 clause there is a choice between different measures. To present this situation without splitting up the clause into too many individual measures RiskCAT uses the Key-Word "***OR***" in its presentation.

To a certain extent again within a single IEC 61508 clause several measures are required, e.g. several documents. To present this situation without splitting up the clause into too many individual measures RiskCAT may give some of the measures (the most important ones, hopefully) ending up with "**…**".

6.4 About the Safety Integrity Level (SIL)

The IEC 61508 provides several approaches to determine the Safety Integrity Level to be required for an E/E/PES.

CAUTION: Using these approaches you should be aware that they are informative only. So it is not appropriate to base decisions about sufficiency of a certain SIL on these approaches merely.

[5] The original clause is in German language. Because no official translation has been available this translation is by CATS.

RiskCAT supports IEC 61508 by implementation of two of these informative approaches:

- a probabilistic (quantitative) approach according to IEC 61508, part 5, Annex C.
- the Risk Graph approach according to IEC 61508, part 5, Figure D.2 and Table D.1

CAUTION: Please be aware that there is a different Risk Graph approach provided by IEC 61508, part 5, **Figure D.1**.

6.4.1 Safety Integrity Level in the Risk Graph Approach

Below SIL 1 the IEC 61508 (part 5, figures D.1 and D.2) denotes the SILs as "No safety requirements" and "No special safety requirements". Instead of this wording RiskCAT uses SIL 0. However, the wording of the standard is presented in addition to the SIL number.

Beyond SIL 4 the IEC 61508 (part 5, figures D.1 and D.2) denotes the SIL as "A single E/E/PES is not sufficient" or "An E/E/PE SRS is not sufficient". In addition to this wording RiskCAT chooses SIL 4.

6.4.2 Safety Integrity Level in the Probabilistic Approach

Table 3 of IEC 61508, part 1, is the basis for the probabilistic approach with RiskCAT. It is restricted to a variation of the probability of a dangerous failure to 4 orders of magnitude from $\geq 10^{-9}$/hour to $<10^{-5}$/hour. In case the rate of dangerous failures may be $\geq 10^{-5}$/hour or needs to be $<10^{-9}$/hour IEC 61508 does not provide any SIL.

RiskCAT results in SIL 0 if the rate of dangerous failures may be $\geq 10^{-5}$/hour.

RiskCAT results in SIL 4 if the rate of dangerous failures needs to be $<10^{-9}$/hour and denotes the SIL as "SIL not valid".

6.4.3 Safety Integrity Level 0

RiskCAT developers feel that there is no clear prescription within IEC 61508 about the degree of obligation of the required measures below SIL 1. So RiskCAT for SIL 0 assigns the lowest degree of obligation which is 'possible' to all measures. In case user feels this approach to be too weak it is suggested to increase the SIL manually from 0 to 1.

6.5 About part 1 of the standard

Requirements within **Part 1** - General Requirements - are independent of SIL except three requirement. It is presented in RiskCAT tab 'Assessment'. Part 1 does not make use of alternative requirements offering the possibility to choose between different approaches.

Within Part 1 there are requirements requiring that part 2 or 3 or certain clauses of those parts shall be applied. This type of requirement has been skipped for purpose of RiskCAT.

Actual database for part 1 is based on pdf file dated 10.08.1999, size 643 897 Bytes containing the 'First edition' of the standard dated '1998-12'. That pdf includes the contents of the corrigendum 1 of April 1999.

Most Part 1 requirements are from clause 7, Overall safety lifecycle requirements. RiskCAT presents these requirements in its area

- "1b: Control System in relation to the EUC"

All other Part 1 requirements are presented in RiskCAT area

- "1a: General".

6.6 About part 2 of the standard

Part 2 - which is about system requirements - makes use of SIL dependent requirements in 8 tables of its annexes which are about selection of techniques and measures. Alternative requirements offering the possibility to choose between different techniques and measures are used in these tables to some extent as well. RiskCAT presents those alternative sets of measures by grey shaded background.

Within Part 2 there are requirements requiring that part 1 or certain clauses of this part shall be applied. This type of requirement has been skipped for purpose of RiskCAT.

Tables A.16 to A.18 as well as B.1 to B.5 besides the importance require a certain SIL dependent effectiveness. Effectiveness requirements are special for part 2. They are not presented in actual RiskCAT version.

The measures grouping in tables B.1 and B.4 as well as second grouping in table B.5 with the opportunity to choose just one method are valid only for 'R' measures. Choice is not allowed for 'HR' measures. Again this importance related grouping is special for part 2. It is not presented in actual RiskCAT version.

Actual database for part 2 is based on file dated 06.11.2000, size 919 951 Bytes containing the 'First edition' of the standard dated '2000-05'. All requirements contained in part 2 are given in clause 7, Lifecycle requirements on the E/E/PES.

On the one hand side these requirements are concerned with the control system as a whole (hardware plus software). These requirements are presented in RiskCAT area

- "2a. Control System".

On the other hand side these requirements are concerned just with the hardware only. These requirements are presented in RiskCAT area

- 2b. Hardware

Capturing the required measures from IEC 61508, CATS felt that in part 2 there are three areas of weaknesses:

- It has been understood that IEC 61508 uses *"failure"* for the effect that E/E/PES does supply its specified function. and it has been understood that IEC 61508 uses *"random failure"* for the physical transition of a hardware device to defect. However, in several cases feeling was that *"failure"* has been used instead of *"random failure"*. For the RiskCAT measures a clear distinction between *"failure"* and *"random failure"* has been tried.
- Most clauses of IEC 61508, part 2, are valid for the E/E/PES as a whole. Others are valid just for the hardware part. For the RiskCAT measures a clear distinction between those two areas of validity has been tried by assigning them to the two areas "3. Control System" and "4. Hardware".
- With respect to integration tests
  - Part 1, Table A.2, mentions "Specification (integration tests of programmable electronic and non programmable electronic hardware)". In part 2, 7.5.2, neither the document is mentioned nor a related activity.
  - Part1, Table A.2 mentions "Specification (hardware architecture integration tests)". In part 2, 7.5.2, neither the document is mentioned nor a related activity.
  - Part 2, 7.4.2.11, suggests that an „E/E/PES integration tests specification" should exist which is suggested by 7.5.2.1 as well. However, this spec is not contained in Part1, Table A.2
  - as a conclusion RiskCAT uses
    * E/E/PES integration tests specification.
    However, it does not use
    * Specification (integration tests of programmable electronic and non programmable electronic hardware)"

6.7 About part 3 of the standard

As part 2 the **part 3** - which is about software requirements - makes extensive use of SIL dependent requirements in its annexes which are about selection of techniques and measures. Alternative requirements offering the possibility to choose between different techniques and measures are used in annexes to some extent as well. RiskCAT presents those alternative sets of measures by grey shaded background.

Actual database for part 3 is based on pdf file dated 10.08.1999, size 537 549 Bytes containing the 'First edition' of the standard dated '1998-12'. That pdf includes the contents of the corrigendum 1 of April 1999.

Most Part 3 requirements are from clause 7, Software safety lifecycle requirements. RiskCAT presents these requirements in its areas

- "3c. Software, Design and development (D+D)" and
- "3b. Software, Lifecycle, but not D+D".

All other Part 3 requirements are presented in RiskCAT area

- "3a. Software, Non Lifecycle".

The Tables of Part 3, Appendix A, are not refining a special requirement but provide techniques and measures for a whole chapter of the standard. So to ease overview and keep low the number of topic tabs the contents of the tables from Appendix A are presented together with the main part requirements as far as they are concerned with just one chapter. However, to provide the possibility of easy identification of the techniques / measures from the appendix they are preceded by a "- ".

To increase clarity RiskCAT 61508 is listing the three measures by Table B.6, „Performance testing", twice. They are listed as well in area "3b. Software, Lifecycle, but not D+D" as in area "3c. Software, Design and development (D+D)".

6.8 About the other parts of the standard

Part 5 - which is about the determination of safety integrity levels - does not involve any requirement. However extensive use has been made of this part in realizing the group box 'IEC 61508 risk'. Therefore RiskCAT offers the opportunity to access the part if related PDF file is available.

Part 4 is about terms only. It is used by RiskCAT for purpose of the context related presentation of terms (see 4.16, "The context related presentation of terms used in the measure texts given in IEC 61508, part 4"; Normal Package only).

Part 6 and **part 7** are examples and explanations. They are used by RiskCAT for purpose of the context related presentation of explanations, especially part 7 (see 4.15, "The context related presentation of explanations to the clause provided by IEC 61508 itself"; Normal Package only). Again RiskCAT offers the opportunity to access the part if related PDF file is available.

6.9 Abbreviations

Abbreviations used in CATS database of IEC 61508:

ALARP	As low as reasonably practicable
DB	Database
D+D	Design and development
E/E/PES	Electrical / electronic / programmable electronic system
EUC	Equipment under control
HW	Hardware
IF	see chapter 6.3, "About some Key-Words in the individual measure presentation in RiskCAT"
OR	see chapter 6.3, "About some Key-Words in the individual measure presentation in RiskCAT"
SFC	Systematic faults control
SIL	Safety integrity level
SW	Software
V+V	Verification and validation
…	see chapter 6.3, "About some Key-Words in the individual measure presentation in RiskCAT"

7 Appendix

7.1 List of Documents

RiskCAT takes the documents listed as examples in IEC 61508, Part 1, tables A.1, A.2 and A.3 (pages 103, 105, 107) as presented in the following table.

The names used in these tables partly have been slightly modified, e.g. "Plan (safety)" from table A.1 to "Overall safety plan" in RiskCAT.

The documents in colour are documents in pairs:

- Yellow plans are related to green reports (and one log)
- Cyan plans and specifications are related to magenta reports

Some of the documents listed in tables A.1, A.2 and A.3 are not addressed by the IEC 61508 measures (and such not by RiskCAT as well). Those are marked by ☹.

Lines on beside the table indicate related pairs of documents.

Document	Table
Overall safety plan Overall verification plan Overall functional safety assessment plan Overall concept description Overall scope description Hazard and risk analysis description Overall safety requirements specification, comprising • Overall safety functions requirements specification and • Overall safety integrity requirements specification Safety requirements allocation description Overall operation and maintenance plan Overall validation plan Overall installation plan Overall commissioning plan	A.1
E/E/PES safety plan E/E/PES verification plan E/E/PES functional safety assessment plan ☹ (for the related clauses please refer to Overall functional safety assessment plan) E/E/PES safety requirements specification, comprising: • E/E/PES safety functions requirements specification and • E/E/PES safety integrity requirements specification E/E/PES validation plan E/E/PES architecture design description, comprising: • HW architecture design description and • SW architecture design description E/E/PES integration tests specification (integration of programmable electronic and non programmable electronic hardware to E/E/PES)	A.2

Document		Table
Hardware (from Table A.2)	*Software (from Table A.3)*	
	SW safety plan SW verification plan SW functional safety assessment plan ☹	
PE integration tests specification ☹ HW architecture design description HW architecture integration tests specification ☹ (no report to this spec in A.2) HW module design specification HW modules test specification ☹ HW modules ☹ HW modules test report ☹ PE integration test report ☹	SW safety requirements specification, comprising: • SW safety functions requirements specification and • SW safety integrity requirements specification SW validation plan PE integration tests specification SW architecture design description SW architecture integration tests specification Development tools instruction ☹ Coding manual SW system design description SW system integration tests specification SW module design specification SW module tests specification Source code list Code review report ~~SW module test report~~ [6] SW module test report SW module integration test report SW system integration test report ☹ SW architecture integration test report ☹ PE integration test report SW validation report	
	SW user instruction SW operation and maintenance instruction SW modification procedures instruction SW modification request SW modification impact analysis report SW modification log SW verification report SW functional safety assessment report ☹	
E/E/PES integration test report (programmable electronic and other hardware integration test) E/E/PES user instruction E/E/PES operation and maintenance instruction E/E/PES validation report E/E/PES modification procedures instruction E/E/PES modification request ☹		A.2

[6] The SW module test report is the only document mentioned twice in IEC 61508, part 1, table A.3. In IEC 61508, part 3, table 1 it is only mentioned as result of the Software module testing. However it is not mentioned as result of code implementation. So for purpose of clearness it has been deleted here as a result of code implementation.

Document	Table
E/E/PES modification impact analysis report E/E/PES modification log E/E/PES verification report E/E/PES functional safety assessment report ☹ (for the related clauses please refer to Overall functional safety assessment report)	
Overall installation report Overall commissioning report Overall validation report Overall operation and maintenance log Overall modification and retrofit • request • impact analysis report • log Overall decommissioning or disposal • impact analysis report • plan • log Overall verification report Overall functional safety assessment report	A.1

For RiskCAT following documents have been added to those given by IEC 61508 :

- QM System
- Component
- Code:Machine
- Overall modification and retrofit procedures instruction (because of part 1, clause 6.2.1.l)
- All
- NA (not applicable)

7.2 List of Activities

RiskCAT takes the activities listed as examples in IEC 61508, Part 1, tables A.1, A.2 and A.3 (pages 103, 105, 107) as presented in the following table.

<table>
<tr><th colspan="2">Activity</th><th>Table</th></tr>
<tr><td colspan="2">Concept
Overall scope definition
Hazard and risk analysis
Overall safety requirements
Safety requirements allocation
Overall operation and maintenance planning
Overall validation planning
Overall installation and commissioning planning
Realisation (see tables A.2 and A.3)</td><td>A.1</td></tr>
<tr><td colspan="2">E/E/PES safety requirements
E/E/PES validation planning
E/E/PES design and development
E/E/PES architecture</td><td>A.2</td></tr>
<tr><td>From Table A.2</td><td>From Table A.3</td><td></td></tr>
<tr><td>Hardware architecture

Hardware module design
Component construction and/or procurement</td><td>Software safety requirements
Software validation planning
Software design and development
Software architecture
Software system design
Software module design
Coding
Software module testing
Software integration</td><td></td></tr>
<tr><td>Programmable electronic integration</td><td>Programmable electronic integration
Software operation and maintenance procedures
Software safety validation
Software modification</td><td></td></tr>
<tr><td colspan="2">E/E/PES integration
E/E/PES operation and maintenance procedures
E/E/PES validation
E/E/PES modification</td><td>A.2</td></tr>
<tr><td colspan="2">Overall installation and commissioning
Overall validation
Overall operation
Overall maintenance
Overall modification and retrofit
Decommissioning or disposal</td><td>A.1</td></tr>
<tr><td colspan="2">All phases</td><td></td></tr>
</table>

For RiskCAT following activities have been added to those given by IEC 61508 :

- Assess
- Conform
- Manage Documents
- Manage Safety
- Reliability Computation
- Review
- NA (not applicable)